U.S. Departmentof Health and Human Services

Sponsored by Secure One HHS

SECURE ONE HHS
KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

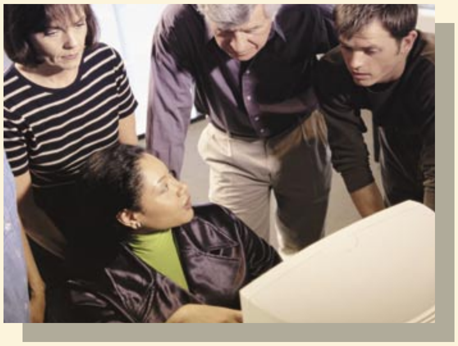
Quick Guide to Information Security

HHS Information Security Program

Secure One HHS was established to promote a Department-wide Information Security Program. Its mission is to foster an enterprise-wide secure and trusted environment in support of HHS' commitment to better health and well-being of the American people. Visit the Secure One HHS intranet site at http://intranet.hhs.gov/infosec/ for the latest information.

It is the responsibility of all Federal employees, contractors, students, guest researchers, visitors, and others who may need access to Federal information systems to comply with laws, regulations, and policies. Please familiarize yourself with the HHS Information Security Program Policy, Handbook, and guidance documents located at http://intranet.hhs.gov/infosec/policies_guides.html. In addition, your Operating Division (OPDIV) and Office/Center have specific policies and procedures that apply to you. Please consult your supervisor or Information System Security Officer (ISSO) for additional security policies and procedures.

Non-compliance with Departmental and OPDIV security policies, procedures, and guidelines may be subject to disciplinary action.



Employee and Visitor Access

- Challenge strangers that do not have a valid employee or visitor badge or an escort
- Report unusual activity to your supervisor, ISSO, or physical security office
- Wear your employee or visitor badge at all times
- Protect your employee or visitor badge and do not loan it to anyone
- Do not permit entry to someone without an employee or visitor badge
- Obey security guards

Work Space Protection

- Lock your computer before you step away from your desk (press CTRL + ALT + DEL)
- Secure your computer with a password-protected screen saver
- Restrict visitor's view of information on your desk and computer monitor
- Keep food and beverages away from your computer
- Protect removable media and portable resources (e.g., laptop, PDA, memory stick)
- Use an uninterrupted power supply
- Log out or shut down your computer at the end of the day, as required by your OPDIV

Password Protection

Ensure that the password:

- Is a minimum of 8 characters
- Contains at least one uppercase letter, one lowercase letter, and one number
- Has no sequentially repeated characters
- Is not a dictionary word
- Is not a term associated with you (e.g., child or pet's name or user ID)
- Is not written down
- Is changed at least every 90 days
- Is never shared

Check with your ISSO for specific password guidance that pertain to your OPDIV, Center, or Office.

Use an easily remembered phrase, and substitute letters and numbers for some words.

Example:

Security is my responsibility at HHS too
S i m R Y a h 2

New password=**SimRYah2**
(This password cannot be used since it has been used here as an example.)

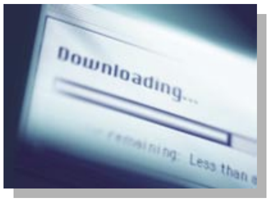
Social Engineering Protection

- Do not give out your username and password
- Dispose of sensitive information properly (e.g., shredding paper documents, disposing paper documents in a secure bin)
- Do not give out your mother's maiden name and social security number over the phone, internet, e-mail, etc.

E-mail Usage

- Ensure your use of e-mail does not harm the mission of HHS or your OPDIV and does not conflict with laws, regulations, and policies
- Report malicious/spam e-mails to your Help Desk or ISSO
- Scan attachments before opening
- Do not open unknown e-mails and attachments
- Be careful when using "reply all" function
- Use discretion when sending e-mail messages and attachments—they are considered official Department documents
- Do not use e-mail to distribute files that are obscene, pornographic, threatening, or harassing
- Do not forward chain letters
- Do not circulate virus warnings not issued by the Department or your OPDIV
- Do not expect privacy
- Empty the "Deleted Items" folder periodically

Internet Usage



- Ensure your use of the Internet does not harm the mission of HHS or your OPDIV and does not conflict with laws, regulations, and policies
- Do not use Internet games and chat rooms
- Do not use the Internet for gambling
- Remove temporary Internet files periodically
- Do not use peer-to-peer file sharing software or functionality

Resource Usage

- Do not use another person's account or identity
- Do not access or attempt to break into another computer (federal or private)
- Do not introduce malicious code (e.g., computer viruses, worms, or Trojan horses)
- Do not send, retrieve, view, display, or print sexually explicit, suggestive text or images, or other offensive material

U.S. Departmentof Health and
Human Services

Sponsored by
Secure One HHS

SECURE ONE HHS
KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Quick Guide to Information Security

Information and Data Protection

- Ensure data is marked with the proper sensitivity level (e.g., For Internal Use Only), check with your ISSO for proper data marking
- Ensure printed material is appropriately stored when not in use
- Ensure classified data is handled properly
- Do not discuss sensitive information in public places
- Protect sensitive files with a password
- Dispose of documents properly (e.g., shredding paper documents, disposing documents in a secure bin)
- Dispose of media properly (e.g., turn in used CD-ROMs, floppy disks, memory sticks to your local Help Desk)
- Contact the Office of Security and Drug Testing (OSDT) if you handle classified data. Also contact your ISSO for OPDIV specific procedures on handling classified data

Data Backup and Media Storage

- Store critical files on the network where they are automatically backed up and available for recovery, if needed
- Back up critical files to a diskette, tape, or CD regularly
- Ensure backup media have adequate space and work properly
- Label backup with date, sensitivity level, and content
- Keep printed copies of critical data

Hardware and Software Usage

- Protect handheld devices (e.g., laptop, PDA, cell phone). Do not leave unattended; lock up or hide when not in use
- Obey software license restrictions
- Do not copy software
- Do not install or download unauthorized software
- Do not connect unauthorized hardware to your computer or network
- Report lost or stolen equipment immediately to your ISSO or Help Desk
- Do not use government equipment to run a personal business

Incident Response

If you think your system is infected with a virus:

1. Stop—do NOT turn off your computer or answer any prompts
2. Take notes—include what happened, the program used, file name, symptoms, and messages or warnings received
3. Get help—contact your Help Desk, ISSO, or System Administrator immediately
4. Be patient—do NOT try to fix the problem yourself

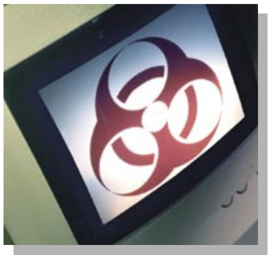
Some viruses are hoaxes, but leave that up to your System Administrator to determine.

Privacy Protection

- Complete privacy training if you handle personal information;* contact your ISSO for more details
- Protect personal information from unauthorized disclosure or damage to help prevent identity theft
- Familiarize yourself with a site's privacy policy before you submit your personal information to the web
- Do not provide personal or financial information through e-mail or pop-up windows

** Personal information includes, but is not limited to, social security numbers and personal health information of HHS employees and the public.*

Virus and Spyware Protection



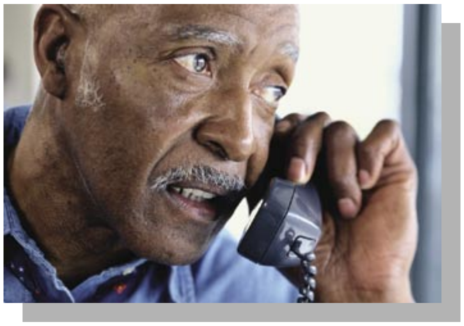
- Scan your computer for viruses, spyware, etc., regularly
- Update virus definitions regularly
- Do not click on links within pop-up windows

Phishing Protection

- Ensure a website has "https" and a padlock before providing personal information
- Contact your Help Desk or ISSO before providing personal information if you are not sure about the request or the validity of the website
- Do not click on hyperlinks within e-mails if you suspect the message is not authentic
- Do not give people or businesses your password, login name, social security number, or other personal information through e-mails
- Examine a site's web address carefully
- Be suspicious of any e-mail with an urgent request for personal or financial information

Security and Privacy Awareness Training

Be sure to complete Security Awareness Training before being granted permanent system and network access. Also, remember to complete refresher Security Awareness Training annually to prevent loss of system and network access. Contact your ISSO for more details.



My Help Desk contact information is:

Telephone Number:________________________

Location:________________________

My ISSO is:________________________

(Primary)
Telephone Number:________________________

(Alternate)
Telephone Number:________________________

OSDT Contact:_

http://intranet.hhs.gov/osdt

Office of Inspector General (OIG)

OIG Hotline: 1-800-HHS-TIPS
www.oig.hhs.gov/hotline.html
Report suspected fraud, waste, or abuse of Departmental programs.

Version July 2005

Administration for Children & Families AHRQ AoA CDC CMS FDA HRSA OS PSC SAMHSA